REMARKS/ARGUMENTS

Favorable reconsideration of this application, in light of the following discussion is respectfully requested.

Claims 1-4 and 11-14 remain active in this case, and stand finally rejected under 35 USC 103 as being unpatentable over Ugon et al. (U.S. Patent No. 6,839,849, hereinafter called "Ugon") in view of Feyt et al. (U.S. Patent No. 6,698,662 , hereinafter called "Feyt").

Applicant respectfully traverses the outstanding rejection because in Applicant's view, the cited references clearly do not obviate the claimed invention.

In particular, the present invention is directed to a data processing apparatus and a memory card, wherein a pseudo data generating circuit is provided so as to generate and output to a data bus pseudo data. As stated in Claims 1 and 11, the pseudo-data generating circuit generates pseudo-data and outputs the pseudo-data to said data bus in a time interval between a read cycle period and a write cycle period, between a write cycle period and a read cycle period, between two read cycle periods, or between two write cycle periods. As stated in Claims 3 and 13, the pseudo-data generating circuit is connected to a control signal generating circuit so as to receive a control, and generates and outputs the pseudo-data to said data bus in accordance with the control signal.

In evaluating the claimed invention, it should be understood that the conventional data processing apparatus makes a slight difference in power consumption in accordance with a change in data on a data bus. The change in the data on the data bus is defined as the number of bits changing from 1 to 0 or from 0 to 1. This difference in power consumption is understood by reference to the attached reference FIG. 1 which shows a case where data on the data bus is comprised of 8 bits.

In FIG. 1, the greater a waveform of the consumed current is, the larger the amount of current will be, and the more data changes, the larger the amount of current is consumed. In FIG. 1, "FFH" indicates an intermediate data of a code using a secret key (secret data). When "00H" and "55H" which are before and after "FFH" are fixed data (read data from a memory), a measured consumed current of changed plain text to be input (data to be encrypted) shows the difference of data changing, and the secret key can easily be known.

On the other hand, reference FIG. 2 shown in the attachment relates to the present invention. In the example shown in FIG. 2, pseudo-data is output to the data bus in a time interval between two cycle periods such as the read cycle period and the write cycle period so that data changing before and after the cycle periods varies. If the waveform of consumed current is averaged, the data changing will also be averaged. Thus, the data changing cannot be known based on the current consumption.

FIG. 2 shows a case where data on the data bus is comprised of 8 bits. When the data is changed from "00H" to "random number," the bit is changed from 0 to 1, or the bit is not changed. The probability of data changing in bit is 1/2, and the average of data changing in 8-bit data bus will be 8 bits x 1/2 = 4 bits. Then, the all average of data changing will be 4 bits, and thus, data changing cannot be known based on the average consumed.

As explained in the Amendment filed August 12, 2005, Ugon does not disclose a pseudo-data generating circuit which generates and outputs pseudo-data to a data bus. Indeed, Ugon at column 11, lines 14- discloses that outputs from a random generator (R1), a register (R2) and a timer (R3) are supplied to a CPU 1 through an interrupt system 15. However, the outputs from the generator (R1), the register (R2) and the timer (R3) are not supplied to a bus (3, 4), as acknowledged at page 3, lines 12-16 of the outstanding Official Acton.

In an effort to remedy this deficiency in Ugon, the outstanding Official Action relies on column 2, lines 36-42 and column 3, lines 34-52 of Feyt, stating "Feyt et al. (6,698,662) teaches presenting a random data items on the data bus during cryptographic calculation like read and write operations." However, Feyt likewise does not teach to output the random data items to the data bus. Instead, Feyt discloses that a current consumption I_{out} of an electronic chip 10 is changed in accordance with operations of a central unit 12 or a memory 14 so as to hide an operation of microprocessor card. The random signal generator 28 in FIG. 1 of Feyt does not output the random data items to the data bus provided between the central unit 12 and the memory 14. That is, Feyt applies a random current noise to a power supply conductor 22 connected to the central unit 12 and the memory 14. Clearly, the power supply conductor 22 is NOT a data bus, and thus this teaching clearly does not remedy the deficiency in Ugon.

Furthermore, while the application of random current noise, as taught by Feyt, may result in an instantaneous variation of the current consumption waveform, if a number of waveforms of consumed current are averaged, the "randomness" in the current waveform introduced by the injected current noise is lost over multiple cycles, such that the random current consumption noise shows a fixed value, as shown in reference FIG. 3. In fact, the average waveform of consumed current will show a waveform obtained by adding a certain value to the waveform of reference FIG. 1. Therefore, the difference of data changing on the data bus is shown by averaging the waveform, and the secret key may be then be derived. Also, Feyt shows an embodiment of stabilizing the current consumption, and does not show it in detail.
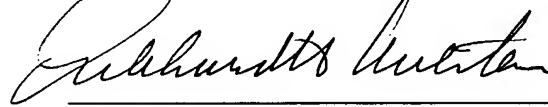
Accordingly, as is believed to be evident from the above discussion, the combined teachings of Ugon and Feyt fail to teach generation and application of pseudo-data to a data

4

line, and in fact teach a completely different approach than as claimed. It is respectfully

submitted that these references clearly do not suggest or obviate the claimed invention and

that the claimed invention is patentable over these references.

Consequently, it is respectfully submitted that the outstanding ground for rejection has

been traversed and that Claims 1-4 and 11-14 clearly define allowable subject matter. An

early and favorable action to that effect is therefore respectfully requested.
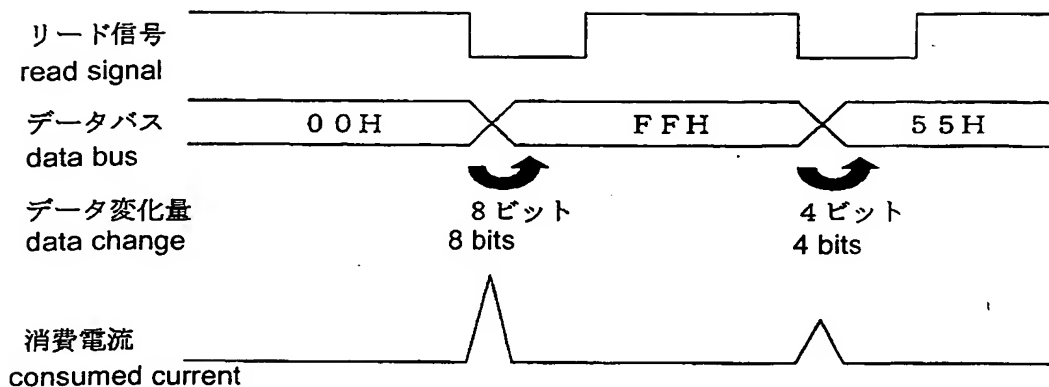
Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
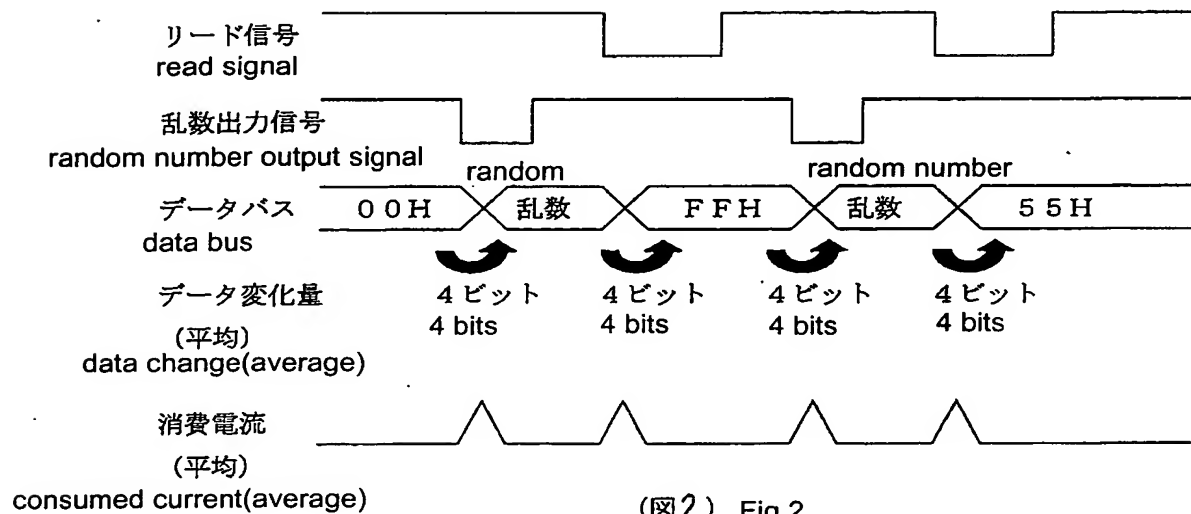MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870
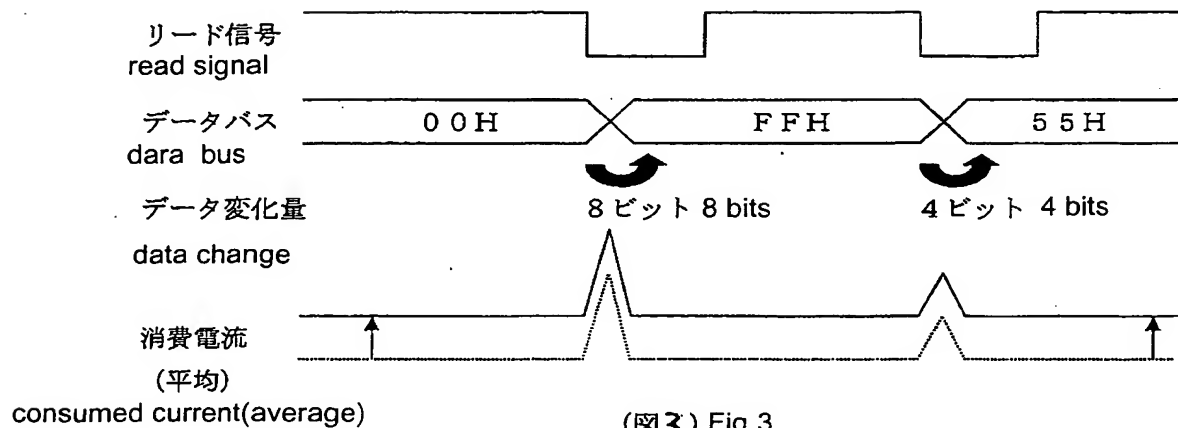
Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\EHK\21'S\217781US\217781US-REQUESTFORRECONSID-4.7.06.DOC

5

リード信号
read signal

データバス
data bus | 0 0 H | F F H | 5 5 H

データ変化量
data change

8 ビット
8 bits

4 ビット
4 bits

消費電流
consumed current

（図1） Fig.1

リード信号
read signal

乱数出力信号
random number output signal

データバス
data bus | 0 0 H | 乱数 random | F F H | 乱数 random number | 5 5 H

データ変化量
（平均）
data change(average)

4 ビット
4 bits

4 ビット
4 bits

4 ビット
4 bits

4 ビット
4 bits

消費電流
（平均）
consumed current(average)

（図2） Fig.2

リード信号
read signal

データバス
dara bus | 0 0 H | F F H | 5 5 H

データ変化量
data change

8 ビット 8 bits

4 ビット 4 bits

消費電流
（平均）
consumed current(average)

（図3） Fig.3